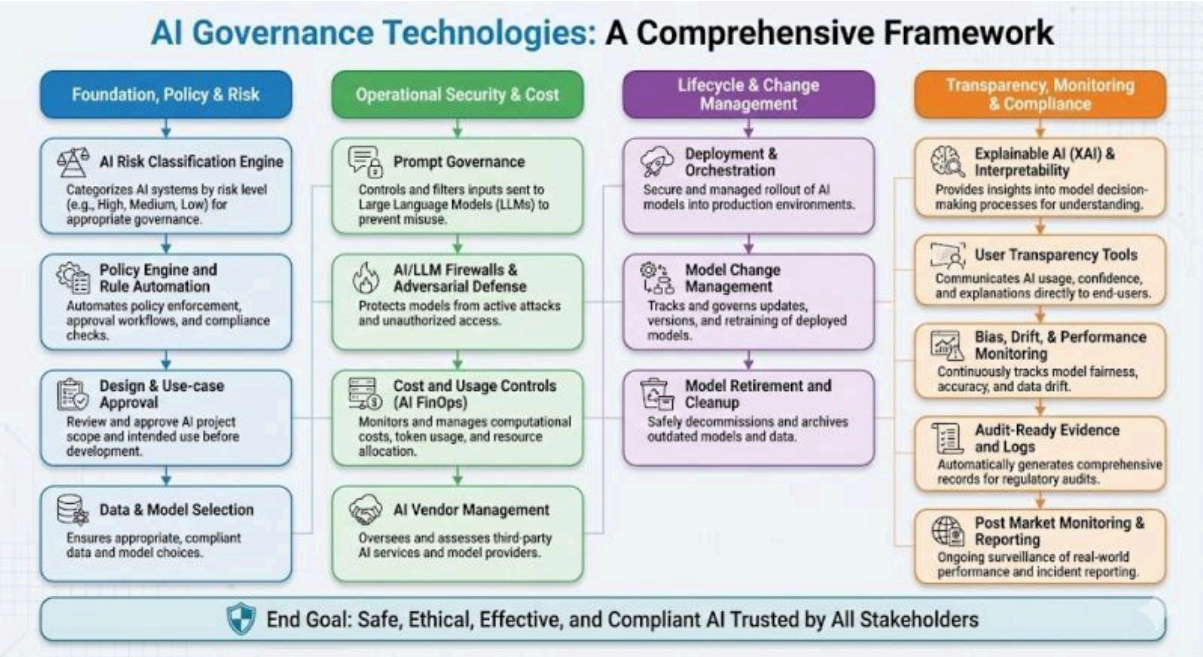
Universidad de Buenos Aires
Facultad de Ciencias Económicas

La Gobernanza de la Inteligencia Artificial

Material de Estudio



🛸 Traducción y Comentarios

Tecnologías de Gobernanza de la Inteligencia Artificial (AI Governance Technologies)

(AI – Artificial Intelligence / Inteligencia Artificial)

1. Fundamentos, Políticas y Riesgo

Motor de Clasificación de Riesgo de IA

(AI Risk Classification Engine)

- Clasifica los sistemas de IA según su nivel de riesgo (por ejemplo: alto, medio, bajo).
- Permite aplicar distintos niveles de control y gobernanza según el impacto del sistema.

Motor de Políticas y Automatización de Reglas

(Policy Engine and Rule Automation)

- Automatiza la aplicación de políticas internas.
- Aprueba flujos de trabajo y verifica el cumplimiento normativo (*compliance*).

Diseño y Aprobación de Casos de Uso

(Design & Use-Case Approval)

- Revisa y aprueba el alcance del proyecto y el uso previsto del sistema antes del desarrollo.
- Asegura alineación con objetivos del negocio y riesgos aceptables.

Selección de Datos y Modelos

(Data & Model Selection)

- Garantiza que los datos y modelos utilizados sean apropiados y cumplan con normas legales y éticas.
- Reduce riesgos de sesgo y uso indebido de información.

---

2. Seguridad Operativa y Costos

Gobernanza de Prompts

(Prompt Governance)

- Controla y filtra los *prompts* (instrucciones) enviados a los modelos de lenguaje.
- Evita usos indebidos o no autorizados de **LLMs** (*Large Language Models – Modelos de Lenguaje de Gran Tamaño*).

Firewalls de IA y Defensa contra Ataques Adversarios

(AI/LLM Firewalls & Adversarial Defense)

- Protege los modelos frente a ataques activos y accesos no autorizados.
- Refuerza la seguridad de los sistemas de información basados en IA.

Control de Costos y Uso (FinOps de IA)

(AI FinOps – Financial Operations / Operaciones Financieras)

- Supervisa costos computacionales, uso de tokens y consumo de recursos.
- Permite una gestión eficiente del presupuesto tecnológico.

Gestión de Proveedores de IA

(AI Vendor Management)

- Evalúa y controla servicios de IA provistos por terceros.
- Analiza riesgos, cumplimiento y dependencia tecnológica.

---

3. Ciclo de Vida y Gestión del Cambio

Despliegue y Orquestación

(Deployment & Orchestration)

- Implementa los modelos de IA de forma segura en entornos productivos.
- Coordina versiones, entornos y dependencias técnicas.

Gestión de Cambios del Modelo

(Model Change Management)

- Registra y gobierna actualizaciones, versiones y reentrenamientos.
- Facilita trazabilidad y control en sistemas productivos.

Retiro y Limpieza de Modelos

(Model Retirement and Cleanup)

- Desactiva modelos obsoletos.
- Archiva datos y versiones antiguas de forma segura.

---

4. Transparencia, Monitoreo y Cumplimiento

IA Explicable e Interpretabilidad

(XAI – Explainable Artificial Intelligence / Inteligencia Artificial Explicable)

- Hace comprensibles los procesos de decisión del modelo.
- Facilita la supervisión gerencial y la rendición de cuentas.

Herramientas de Transparencia para Usuarios

(User Transparency Tools)

- Comunican a los usuarios cómo funciona la IA.
- Explican niveles de confianza y resultados generados.

Monitoreo de Sesgos, Deriva y Desempeño

(Bias, Drift & Performance Monitoring)

- Detecta cambios en precisión, equidad y calidad de los datos.
- Permite ajustes tempranos antes de impactos en el negocio.

Evidencia y Registros de Auditoría

(Audit-Ready Evidence and Logs)

- Genera automáticamente documentación para auditorías regulatorias.
- Asegura trazabilidad y cumplimiento normativo.

Monitoreo y Reportes Post-Implementación

(Post-Market Monitoring & Reporting)

- Supervisa el desempeño real del sistema en producción.
- Reporta incidentes y riesgos emergentes.

Objetivo Final

- Lograr una **IA segura, ética, eficaz y en cumplimiento normativo**, confiable para todas las partes interesadas (*stakeholders*), integrando adecuadamente la gobernanza dentro de los **sistemas de información y procesos organizacionales**.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.